RP-150: Formulation of solutions of a very special class of standard quadratic congruence of composite modulus modulo an even- prime of even power

Prof B M Roy

Head, Department of Mathematics
Jagat Arts, Commerce & I H P Science College, Goregaon
Dist Gondia. M. S., India. Pin: 441801.

***Abstract*: In this paper, the author has formulated a very special type of standard quadratic congruence of even composite modulus modulo an even prime of even power. The established formula for solutions of the congruence is tested and verified true. The formula proves time-saving and simple. No such formula is found in the literature of mathematics. First time the author has formulated the solutions of the congruence. This formulation makes the study of quadratic congruence very interesting and simple. Formulation of solutions is the merit of the paper.**

***Keywords*: Composite modulus, Formulation, Incongruent solutions, Quadratic congruence.**

INTRODUCTION
Quadratic congruence of prime & composite modulus is a part of Number Theory. It is found that much had not been researched on the formulation of solutions of the congruence in this field of mathematics. A very less attempts had been taken on the research in this part. The author first time started formulating different standard quadratic congruence. He already has formulated many standard quadratic congruence of composite modulus successfully [1], [2], [3], [4], [5].

PROBLEM-STATEMENT
Here the problem is –"To formulate the solutions of the congruence of the type:

$$x^2 \equiv 2^{2m} \pmod{2^n};\ n \geq 2m+2, n \text{ is even}".$$

LITERATURE REVIEW
The book of Zuckerman [6] has placed an example in its exercise that if

$a \equiv 1 \pmod 8$ and x_0 is any solution of the congruence $x^2 \equiv a \pmod{2^n}$, then the standard quadratic congruence has exactly four incongruent solutions and these four solutions are given by $x_0, -x_0, 2^{n-1}+x_0, 2^{n-1}-x_0$.

Koshy [7] and Burton [8] also consider the same problem in the same manner.
In their consideration, $a \equiv 1 \pmod 8$ means a is an odd positive integer. Nothing is said when a is even and of the type 2^m. So, the author considered the problem for his research in the above form and formulate the solutions of the said congruence.

ANALYSIS & RESULTS
Consider the congruence: $x^2 \equiv 2^{2m} \pmod{2^n}$.
It can be written as: $x^2 \equiv (2^m)^2 \pmod{2^n}$.
Let us consider $x \equiv 2^{n-m-1}k \pm 2^m \pmod{2^n}$.
Then, $x^2 \equiv (2^{n-m-1}k \pm 2^m)^2 \pmod{2^n}$

$$\equiv (2^{n-m-1}k)^2 \pm 2.2^{n-m-1}k.2^m + (2^m)^2 \pmod{2^n}$$
$$\equiv (2^{n-m-1}k)^2 \pm 2^n k + (2^m)^2 \pmod{2^n}$$
$$\equiv 2^n k(2^{n-2m-2}k \pm 1) + 2^{2m} \pmod{2^n};\ \text{if } n \geq 2m+2.$$
$$\equiv 2^{2m} \pmod{2^n}.$$

Thus, $x \equiv 2^{n-m-1}k \pm 2^m \pmod{2^n}$ can be consider as the solution formula for the said congruence. But for $k = 2^{m+1}$, the solution reduces to

$$x \equiv 2^{n-m-1}.2^{m+1} + 2^m \pmod{2^n}.$$
$$\equiv 2^n + 2^m \pmod{2^n}$$
$$\equiv 2^m \pmod{2^n}.$$

This is the same solution as for $k = 0$.
Also for $k = 2^{m+1}+1$, the solution reduces to

$$x \equiv 2^{n-m-1}.(2^{m+1}+1) + 2^m \pmod{2^n}.$$
$$\equiv (2^n + 2^{n-m-1}) + 2^m \pmod{2^n}$$
$$\equiv 2^{n-m-1} + 2^m \pmod{2^n}.$$

This is the same solution as for $k = 1$.
Therefore, it can be seen that all the solutions are given by

$$x \equiv 2^{n-m-1}k \pm 2^m \pmod{2^n};\ k = 0, 1, 2, \ldots\ldots\ldots, (2^{m+1}-1).$$

This gives $2.(2^{m+1}) = 2^{m+2}$ incongruent solutions of the said congruence.

ILLUSTRATIONS

Example-1: Consider the congruence $x^2 \equiv 16 \pmod{256}$.
It can be written as: $x^2 \equiv 2^4 \pmod{2^8}$.
It is of the type: $x^2 \equiv 2^{2m} \pmod{2^n}$ with $n = 8$; $m = 2$.
It has exactly $(2^{m+2}) = 2^4 = 16$ incongruent solutions.
These solutions are given by: $x \equiv 2^{n-2-1}k \pm 2^2 \pmod{2^n}$; k = 0, 1, 2, 3,…….. $(2^{m+1} - 1)$.
Putting the known values:

$$x \equiv 2^{8-3}k \pm 2^2 \pmod{2^8}; k = 0, 1, 2, 3, 4, 5, 6, 7.$$
$$\equiv 2^5k \pm 4 \pmod{256}$$
$$\equiv 32k \pm 4 \pmod{256}$$
$$\equiv 0 \pm 4; 32 \pm 4; 64 \pm 4; 96 \pm 4; 128 \pm 4; 160 \pm 4; 192 \pm 4; 224 \pm 4 \pmod{256}.$$
$$\equiv 4, 252; 28, 36; 60, 68; 92, 100; 124, 132; 156, 164; 188, 196; 220, 228 \pmod{256}.$$

These are the required sixteen incongruent solutions of the above congruence.

Example-2: Consider one more congruence: $x^2 \equiv 64 \pmod{1024}$.
It can be written as: $x^2 \equiv 2^6 \pmod{2^{10}}$.
It is of the type: $x^2 \equiv 2^{2m} \pmod{2^n}$ with $n = 10$ & $m = 3$.
It has exactly $2.(2^{m+1})$ =$2.2^4 = 2.16 = 32$ Incongruent solutions.
These solutions are given by: $x \equiv 2^{n-m-1}k \pm 2^m \pmod{2^n}$; k=0, 1, 2, 3,……$(2^{m+1} - 1)$.
Putting the known values:

$$x \equiv 2^{10-3-1}k \pm 2^3 \pmod{2^{10}}; k = 0, 1, 2, 3, \dots\dots\dots, 14, 15.$$
$$\equiv 2^6k \pm 2^3 \pmod{1024}$$
$$\equiv 64k \pm 8 \pmod{1024}$$
$$\equiv 0 \pm 8; 64 \pm 8; 128 \pm 8; 192 \pm 8; 256 \pm 8; 320 \pm 8; 384 \pm 8;$$
$$448 \pm 8; 512 \pm 8; 576 \pm 8; 640 \pm 8; 704 \pm 8; 768 \pm 8; 832 \pm 8;$$
$$896 \pm 8; 960 \pm 8 \pmod{1024}.$$
$$\equiv 8, 1016; 56, 72; 120, 136; 184, 200; 248, 264; 312, 328; 376, 392;$$
$$440, 456; 504, 520; 568, 584; 632, 648; 696, 712; 760, 776; 824, 840;$$
$$888, 904; 952, 968 \pmod{1024}.$$

These are the required thirty two incongruent solutions of the above congruence.

Example -3: Consider one more congruence: $x^2 \equiv 64 \pmod{1024}$.
It can be written as: $x^2 \equiv 2^8 \pmod{2^{14}}$.
It is of the type: $x^2 \equiv 2^{2m} \pmod{2^n}$ with $n = 14$ & $m = 4$.
It has exactly $2.(2^{m+1})$ =$2.2^5 = 2.32 = 64$ Incongruent solutions.
These solutions are given by: $x \equiv 2^{n-m-1}k \pm 2^m \pmod{2^n}$; k=0, 1, 2, 3,……$(2^{m+1} - 1)$.
Putting the known values:

$$x \equiv 2^{14-4-1}k \pm 2^4 \pmod{2^{14}}; k = 0, 1, 2, 3, 4, 5, 6, \dots\dots\dots, 31.$$
$$\equiv 2^9k \pm 2^4 \pmod{16384}$$
$$\equiv 512k \pm 16 \pmod{16384}$$
$$\equiv 0 \pm 16; 512 \pm 16; 1024 \pm 16; 1536 \pm 16; 2048 \pm 16; 2560 \pm 16;$$
$$\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots. 14848 \pm 18 \pmod{1024}.$$

These are the required sixty-four incongruent solutions of the above congruence.

CONCLUSION

Thus, it can be conclude that the standard quadratic congruence of even composite modulus of the type: $x^2 \equiv 2^{2m} \pmod{2^n}$, $n \geq 2m + 2$ has exactly 2.2^{m+1}i. e 2^{m+2} Incongruent solutions given by
$x \equiv 2^{n-m-1}k \pm 2^m \pmod{2^n}; k = 0, 1, 2, 3 \dots\dots\dots, (2^{m+1} - 1)$.

MERIT OF THE PAPER

The author first time has formulated such a very special type of standard quadratic congruence of composite modulus having a very large number of solutions. Formula established saves the time of calculation of solutions. A large number of solutions can be obtained directly. Therefore, formulation of solutions is the merit of the paper.

REFERENCES

[1] Roy B M, Formulation of solutions of a class of standard quadratic congruence of even composite modulus, International Journal of Science and Engineering Development Research (IJSDR), ISSN: 2455-2631, Vol-03, Issue-08, Aug-18.
[2] Roy B M, Formulation of a special class of standard quadratic congruence of composite modulus-a multiple of an odd integer, International Journal of Scientific research and Engineering Development (IJSRED), ISSN: 2581-7175, Vol-02, Issue-06, Nov-Dec-19.
[3] Roy B M, Formulation of solutions of a special class of standard quadratic congruence of even composite modulus, Research Journal of Mathematical & Statistical Science, (RJMSS), ISSN: 2320-6047, Vol-08, Issue-01, Jan -20.

[4] Roy B M, A Review and reformulation of the solutions of a standard quadratic congruence of even composite modulus- a power of an odd prime, International Journal of Engineering Technology Research and Management (IJETRM), ISSN: 2456-9348, Vol-04, Issue-02, Feb-20.
[5] Roy B M, Formulation of solutions of a very special class of standard quadratic congruence of composite modulus modulo a multiple of powered even prime by a powered odd prime, International Journal of Trends in scientific Research and Development (IJTSRD), ISSN: 2456-6470, Vol-04, Issue-06, Oct-20.
[6] Zuckerman et al, 2008, An Introduction to The Theory of Numbers, Willey India (Pvt) Ltd, Fifth edition(Indian Print), ISBN: 978-81-265-1811-1.
[7] Thomas Koshy, 2009, Elementary Number Theory with Applications, Academic Press, second edition, ISBN: 978-81-312-1859-4.
[8] David M Burton, 2012, Elementary Number Theory, Mc Graw Hill education, Seventh edition, ISBN: 978-1-25-902576-1.